

ABSTRACT

A system and method secure transactional data communicated over a wireless network in a store by obfuscating bona fide transactional messages in the message traffic flow. The system includes a load balancer coupled to a store host computer and a plurality of transactional terminals coupled to the store host computer through a wireless communication network. The load balancer monitors message traffic queues and message processing at the store host computer to determine possible dead time in the bandwidth of the wireless communication network. If the dead time is greater than a threshold, a bogus request message is generated and sent to one or more terminals in the system. In response to receipt of a bogus request message, a terminal activates a bogus message generator. The bogus message generator generates transactional messages with bogus customer, account, and transactional data therein. The generated messages are transmitted to the store host computer until a bogus message timer expires or a bona fide transaction commences at the terminal where the bogus message generator has been activated. To further frustrate would be eavesdroppers, the bogus and bona fide transactional messages are encrypted to increase processing time for the messages by eavesdroppers. The increased message traffic volume camouflages the true communication parameters of the network and makes analysis of the traffic flow by eavesdroppers more difficult.